JOURNAL OF ALGEBRA 140, 355–359 (1991)

# Central Extensions of $S_n$ as Galois Groups of Regular Extensions of $\mathbb{Q}(T)$

JACK SONN

*Technion – Israel Institute of Technology, 32000 Haifa, Israel*

*Communicated by Walter Feit*

Received September 22, 1989

Recently Mestre [Me] has proved that the double cover $\tilde{A}_n$ of the alternating group $A_n$ is realizable as the Galois group of a regular extension of the rational function field $\mathbb{Q}(T)$, for all $n \geqslant 4$. We show here that his method yields the same result for the two double covers $S_n^{\pm}$ of the symmetric group $S_n$, and more generally, for every finite central extension of $S_n$. Partial results on $S_n$ have been obtained previously by several authors [KSS, So1, So2, SS, V].

## 1. PRELIMINARIES

In this section we summarize some of Mestre's results [Me]. Let $n$ be an odd integer $>1$, and let $A = \mathbb{Z}[A_1, ..., A_n]$ with $A_1, ..., A_n$ indeterminates, $K$ the field of fractions of $A$, $\bar{K}$ the algebraic closure of $K$. Let $P(X)$ be the generic polynomial

$$X^n + A_1 X^{n-1} + \cdots + A_n \in K[X].$$

PROPOSITION 1 [Me]. (a) *There exist polynomials $Q(X)$, $R(X) \in A[X]$ such that:*

(i) *$Q$, $R$ are primitive polynomials in $A[X]$*

(ii) *$Q$, $R$ are relatively prime in $A[X]$*

(iii) *$Q$, $R$ have degree $n-1$*

(iv) $PQ' - P'Q = R^2$.

*(Here $P'$, $Q'$ denote the derivatives of $P$, $Q$ with respect to $X$.)*
*$Q$ is unique and $R$ is unique up to sign and has distinct roots in $K$.*

(b) *Let $T$ be a new indeterminate and set*

$$F_T(X) = P(X) - TQ(X) \in A[T, X].$$



0021-8693/91 $3.00

*Then the discriminant of $F_T(X)$ with respect to $X$ is equal to $\Delta(P)S(T)^2$, where $\Delta(P)$ is the discriminant of $P$ and $S(T) \in A[T]$ is of degree $n-1$ and has distinct roots.*

Now let $H$ denote the product of the leading coefficient of $S(T)$ and $\Delta(S)\,\mathrm{res}(P, R)$, where res denotes the resultant. Note that since $S$ has distinct roots, and by (iv), $P, R$ have no common root, $H$ is a nonzero element of $A$.

Let $k$ be a field of characteristic zero. If $\alpha_1, ..., \alpha_n \in k$, the polynomial

$$P_\alpha(X) = X^n + \alpha_1 X^{n-1} + \cdots + \alpha_n$$

is called *H-general* if $H(\alpha_1, ..., \alpha_n) \neq 0$, where $H = H(A_1, ..., A_n)$ is as above. $P_\alpha$ is the polynomial obtained from $P$ by specializing $A_i = \alpha_i \in k$. For fixed $\alpha$, we will drop the subscript $\alpha$ and write $P = P_\alpha$. Similarly we write $Q = Q_\alpha$, $R = R_\alpha$, $S = S_\alpha$ for the corresponding specializations, and $F_T(X) = P(X) - TQ(X) \in k[T, X]$.

PROPOSITION 2 [Me]. *Let $P(X) \in k[X]$ be an H-general polynomial of degree $n$, $F_T(X) = P(X) - TQ(X) \in k[T, X]$ the corresponding polynomial by Proposition 1 and specialization into $k$. Then the Galois group of $F_T(X)$ over $k(T)$ is $A_n$ (the alternating group) if $\Delta(P)$ is a square in $k$, and is $S_n$ (the symmetric group) otherwise.*

PROPOSITION 3 [Me]. *Let $P$ be as in Proposition 2, and let $B = k(T)[X]/(F_T(X))$. Then the trace quadratic form $\mathrm{Tr}_{B/k(T)}(x^2)$ is independent of $T$.*

Now suppose $x_1, ..., x_n$ are distinct rational numbers, chosen so that $P(X) = \prod_i (X - x_i) = X^n + \alpha_1 X^{n-1} + \cdots + \alpha_n$ is $H$-general. (To see that such a choice is possible, we observe that $H$ is a nonzero polynomial in the roots $X_i$ of $\sum A_i X^i = \prod (X - X_i)$, and a specialization of the $X_i$ into $\mathbb{Q}$ for which $H \neq 0$ induces one of the $A_i$ into $\mathbb{Q}$ for which $H \neq 0$.) Then the Galois group of $F_T(X)$ over $\mathbb{Q}(T)$ is $A_n$ since $\Delta(P)$ is a square in $\mathbb{Q}$. The corresponding trace form is independent of $T$ by Proposition 3, and for $T = 0$ the trivial form $X_1^2 + \cdots + X_n^2$ is obtained. Hence the Witt invariant vanishes, so by [Se], Mestre concludes: for every odd $n \geq 5$, there exists a regular Galois extension $K$ of $\mathbb{Q}(T)$ with group $\tilde{A}_n$, where $\tilde{A}_n$ is the unique double cover of $A_n$.

If $\xi$ is a root of $F_T(X)$ in $K$, then $T = P(\xi)/Q(\xi)$, so $\mathbb{Q}(T)(\xi) = \mathbb{Q}(\xi)$ is a rational function field, and is the fixed field of $\tilde{A}_{n-1}$ in the above Galois extension for $\tilde{A}_n$. Thus there is a regular Galois extension of $\mathbb{Q}(\xi)$ with Galois group $\tilde{A}_{n-1}$. Thus the result for $n$ even is deducible from the result for $n$ odd.

## 2. Central Extensions of $S_n$

Let $S_n^+$, $S_n^-$ denote the two double covers of $S_n$ (see [So1]).

THEOREM 1. *In order that every central extension of $S_n$ be realizable as the Galois group of a regular extension of $\mathbb{Q}(T)$, it suffices to prove it for all groups of the form*

$$S_3 \times_{C_2} C_{2^m}, \quad m \geqslant 1 \qquad \text{and} \qquad S_n^{\pm} \times_{C_2} C_{2^m}, \quad n \geqslant 4, \quad m \geqslant 1,$$

*where $A \times_C B$ denotes the pullback of $A \to C \leftarrow B$.*

*Proof.* This theorem has been proved in [KSS, Theorem 6] for extensions of a number field $k$ instead of regular extensions of $\mathbb{Q}(T)$. The proof is entirely group-theoretic, except for the following two properties of $k$ that are used:

(1) If a finite group $G$ is realized as a Galois group over $k$ then so is every factor group of $G$.

(2) If $G$ is realized as a Galois group over $k$ then so is $G \times A$ for any finite abelian group $A$.

In order to transfer the proof to $\mathbb{Q}(T)$, we need the following replacements for (1) and (2):

(1′) If a finite group $G$ is realizable as the Galois group of a regular extension of $\mathbb{Q}(T)$, then so is every factor group of $G$.

(2′) If a finite group $G$ is realizable as the Galois group of a regular extension of $\mathbb{Q}(T)$, then so is $G \times A$, for any finite abelian group $A$.

(1′) is clear and (2′) follows from [Ma, Zusatz 1, p. 226].

THEOREM 2. *Let $n$ be a positive integer. Then every finite central extension of the symmetric group $S_n$ is realizable as the Galois group of a regular extension of $\mathbb{Q}(T)$.*

*Proof.* It is known that every finite abelian group is the Galois group of a regular extension of $\mathbb{Q}(T)$ [Ma, p. 224]. We may therefore assume $n \geqslant 3$.

*Case* 1. $n$ odd.

Let $m$ be fixed $\geqslant 2$ (without loss of generality). Let $V$ be an indeterminate, $Z/\mathbb{Q}(V)$ a regular cyclic extension of degree $2^m$. Let $U \in \mathbb{Q}[V]$ be such that $\mathbb{Q}(V, \sqrt{U})/\mathbb{Q}(V)$ is the quadratic subextension of $Z/\mathbb{Q}(V)$. Note that since $m \geqslant 2$, $-1 \in \mathbb{Q}(V)$ is a norm from $\mathbb{Q}(V, \sqrt{U})$ by a theorem of Albert, so the quaternion algebra $(-1, U)$ splits. Let $W$ be a new indeterminate, $k = \mathbb{Q}(V, W)$. Then $k(\sqrt{U})/k$ is the quadratic subextension of $kZ/k$.

Form the quadratic polynomial

$$(X-W-\sqrt{U})(X-W+\sqrt{U})=X^2-2WX+W^2-U$$

and observe that since the coefficients $-2W$ and $W^2-U$ are algebraically independent over $\mathbb{Q}$, so are the two roots of this polynomial. Now let $X_3, ..., X_n$ be new indeterminates and form

$$\begin{aligned}P(X)&=(X^2-2WX+W^2-U)(X-X_3)\cdots(X-X_n)\\&=X^n+B_1X^{n-1}+\cdots+B_n,\end{aligned}$$

where $B_i=B_i(V, W, X_3, ..., X_n)$. Since the roots of $P(X)$ are algebraically independent over $\mathbb{Q}$, so are the coefficients $B_1, ..., B_n$. Hence $H(B_1, ..., B_n)$ is not identically zero as a polynomial in $V, W, X_3, ..., X_n$. We may therefore specialize $X_3, ..., X_n$ into $k$ (into $\mathbb{Q}$ if we wish) to obtain an $H$-general polynomial in $k[X]$ which we will also denote $P(X)$. By Proposition 2, the Galois group of $F_T(X)=P(X)-TQ(X)$ over $k(T)$ is $S_n$ since $\Delta(P)\sim U$ is not a square in $k$. Let $K$ be the splitting field of $F_T(X)$ over $k(T)$. By Proposition 1, $k(T, \sqrt{U})/k(T)$ is the quadratic subextension of $K/k(T)$. Hence

$$G(KZ/k(T))\cong S_n\times_{C_2}C_{2^m}.$$

In the case $n=3$, we now specialize $T, W$ into $\mathbb{Q}(V)$ to obtain a regular extension $L/\mathbb{Q}(V)$ with Galois group $S_3$ and quadratic subextension $\mathbb{Q}(V, \sqrt{U})/\mathbb{Q}(V)$. The composite $ZL$ has Galois group $S_3\times_{C_2}C_{2^m}$ over $\mathbb{Q}(V)$. We will see that $ZL$ is a regular extension of $\mathbb{Q}(V)$. Now let $n>4$. The trace form on $M=k(T)[x]/(F_T(X))$ is equivalent to the form

$$2Y_1^2+2UY_2^2+Y_3^2+\cdots+Y_n^2.$$

The Witt invariant of this form (see [Se]) is then $(2, 2U)=(2, U)$. By Serre's formula [Se], the obstruction to the embedding problem for $S_n^-$ ($\tilde{S}_n$ in Serre's notation) is $(2, U)(2, U)=1$, and the obstruction for $S_n^+$ (the other double cover; see [So1]) is $(2, U)(-2, U)=(-1, U)=1$, as noted above. The quadratic subextension of $K/k(T)$ is $k(T)(\sqrt{U})$, hence $K$ is not a $k$-regular extension of $k(T)$, but is a $\mathbb{Q}$-regular extension of $\mathbb{Q}(V, W, T)=k(T)$. We may now specialize $T, W$ to obtain a regular extension $L^{\pm}/\mathbb{Q}(V)$ with Galois group $S_n^{\pm}$ (here $\pm$ means $+$, $-$, respectively) and with quadratic subextension $\mathbb{Q}(V, \sqrt{U})/\mathbb{Q}(V)$. The composite $ZL^{\pm}$ has Galois group $S_n^{\pm}\times_{C_2}C_{2^m}$ over $\mathbb{Q}(V)$.

We claim $ZL^{\pm}$ is a regular extension of $\mathbb{Q}(V)$. Let $L$ be the subfield of $L^{\pm}$ such that $G(L/\mathbb{Q}(V))\cong S_n$. It suffices to show that $ZL/\mathbb{Q}(V)$ is regular, for otherwise, $S_n^{\pm}\times_{C_2}C_{2^m}$ would be isomorphic to $S_n\times_{C_2}C_{2^m}\times C_2$, which is

not the case since the latter group does not have $S_n^{\pm}$ as a factor group. We now show that $ZL/\mathbb{Q}(V)$ is regular and include the case $n=3$. To see this we can use a group-theoretic argument to show that any proper normal subextension of $ZL/\mathbb{Q}(V)$ must contain $\mathbb{Q}(V, \sqrt{U})/\mathbb{Q}(V)$ which is regular. This assertion is equivalent to saying that every proper normal subgroup of $S_n \times_{C_2} C_{2^m}$ is contained in the subgroup $A_n \times C_{2^{m-1}}$ of index two, i.e., $A_n \times C_{2^{m-1}} = N_0$ is the unique maximal normal subgroup of $G_0 = S_n \times_{C_2} C_{2^m}$. We show this is true for all $n \geqslant 3$. Suppose $N$ is a proper normal subgroup not contained in $N_0$. Then it projects onto $S_n$ and onto $C_{2^m}$, so its commutator subgroup $N'$ projects onto $A_n$. But $N' \subseteq S_n \times \{1\}$ since $C_{2^m}$ is abelian. Hence $N \supseteq A_n \times \{1\}$. It follows that $N = G_0$, contradiction. By Theorem 1, the proof for odd $n$ is complete.

We now turn to the case $n$ even. Returning to the preceding proof for $n$ odd $\geqslant 5$, the subfield $M$ of $K$ generated by a root $\xi$ of $F_T(X)$ is a rational function field $k(\xi)$ since $T = P(\xi)/Q(\xi)$. Moreover $G(K/k(\xi)) \cong S_{n-1}$ and $G(K^{\pm}/k(\xi)) \cong S_{n-1}^{\pm}$. The quadratic subextension of $K^{\pm}/k(\xi)$ is $k(\xi)(\sqrt{U})/k(\xi)$ and the proof proceeds from here exactly as before, with $k(T)$ replaced by $k(\xi)$. Specialize $\xi, W$ into $\mathbb{Q}(V)$ to obtain a regular extension $L^{\pm}/\mathbb{Q}(V)$ with group $S_{n-1}^{\pm}$ and quadratic subextension $\mathbb{Q}(V, \sqrt{U})/\mathbb{Q}(V)$. The composite $ZL^{\pm}$ has group $S_{n-1}^{\pm} \times_{C_2} C_{2^m}$ over $\mathbb{Q}(V)$, and is regular as above. ∎

Hilbert's irreducibility theorem yields

COROLLARY 1. *Every finite central extension of $S_n$ is a Galois group over every number field, for every $n$.*

## REFERENCES


[KSS] D. KOTLAR, M. SCHACHER, AND J. SONN, Central extensions of symmetric groups as Galois groups, *J. Algebra* **124** (1989).

[Ma] B. H. MATZAT, Konstructive Galoistheorie, *in* "Lecture Notes in Math., Vol. 1284, Springer-Verlag, New York, 1987.

[Me] J-F. MESTRE, Extensions regulières de $\mathbb{Q}(T)$ de groupe de Galois $\tilde{A}_n$, preprint.

[Se] J-P. SERRE, L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$, *Comment. Math. Helv.* **59** (1984), 651–676.

[So1] J. SONN, Double covers of $S_5$ and Frobenius groups as Galois groups over number fields, *J. Algebra* **114** (1988), 401–410.

[So2] J. SONN, Central extensions of $S_n$ as Galois groups via trinomials, *J. Algebra* **124** (1989), in press.

[SS] M. SCHACHER AND J. SONN, Double covers of the symmetric groups as Galois groups over number fields, *J. Algebra* **116** (1988), 243–250.

[V] N. VILA, On stem extensions of $S_n$ as Galois groups over number fields, preprint.